Board about such material prior to purchase or as soon as possible.

(e) At the conclusion of each review and, as necessary, the Board shall issue guidance to purchasing agents and managers of retail outlets about the purchase, withdrawal, and return of sexually explicit material. The Board may also provide guidance to purchasing agents and managers of retail outlets about material that it has determined is not sexually explicit. Purchasing agents and managers of retail outlets shall continue to follow their usual purchasing and stocking practices unless instructed otherwise by the Board.

(f) Material which has been determined by the Board to be sexually explicit may be submitted for reconsideration every 5 years. If substantive changes in the publication standards occur earlier, the purchasing agent or manager of a retail outlet under DoD jurisdiction may request a review.

§ 235.7 Information requirements.

The Chair of the Board shall submit to the PDUSD(P&R) an annual report documenting the activities, decisions, and membership of the Board. Negative reports are required. The annual report shall be due on October 1st of each year and is not subject to the licensing internal information requirements of DoD 8910.1–M.[2]

PART 236—DEPARTMENT OF DEFENSE (DOD)-DEFENSE INDUSTRIAL BASE (DIB) VOLUNTARY CYBER SECURITY AND INFORMATION ASSURANCE (CS/IA) ACTIVITIES

Sec.

AUTHORITY: 10 U.S.C. 2224; 44 U.S.C. 3506; 44 U.S.C. 3544.

[2] Copies may be obtained at *http://www.dtic.mil/whs/directives/*.

SOURCE: 77 FR 27618, May 11, 2012, unless otherwise noted.

§ 236.1 Purpose.

Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. DoD's voluntary DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

§ 236.2 Definitions.

As used in this part:

(a) *Attribution information* means information that identifies the DIB participant, whether directly or indirectly, by the grouping of information that can be traced back to the DIB participant (e.g., program description, facility locations).

(b) *Compromise* means disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional, or unintentional, disclosure, modification, destruction, loss of an object, or the copying of information to unauthorized media may have occurred.

(c) *Covered defense information* means unclassified information that:

(1) Is:

(i) Provided by or on behalf of the DoD to the DIB participant in connection with an official DoD activity; or

(ii) Collected, developed, received, transmitted, used, or stored by the DIB participant in support of an official DoD activity; and

(2) Is:

(i) Technical information marked for restricted distribution in accordance with DoD Directive 5230.25, ''Withholding of Unclassified Technical Data From Public Disclosure,'' or DoD Directive 5230.24, ''Distribution Statements on Technical Documents'';

(ii) Information subject to export control under the International Traffic in Arms Regulations (ITAR) (*http://pmddtc.state.gov/regulations_laws/itar_official.html*), or the Export Administration Regulations (EAR) (*http://ecfr.gpoaccess.gov*, Title 15, part 730);